Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Standard to Safeguard Information on Portable Computing and Storage Devices

I. **Statement**

State custodians of electronic information will safeguard classified information stored on portable computer devices (common examples include laptops, pocket personal computers, hand-held devices, USB thumb drives, cell phones etc.) by properly classifying data, using encryption to prevent unauthorized access, and requiring written authority to copy data to portable devices.

II. **Purpose**

To reduce the risk to the State if classified information is compromised, lost or stolen while on a portable device.

III. **Applicability**

This standard applies to data custodian agencies within the Executive Branch and semi-autonomous agencies of Maine State government, and to all their applications and data irrespective of where they are hosted. This standard also extends to those applications owned by all governmental branches that are hosted on computer devices operated by the Office of Information Technology or that traverse the State's wide area network.

IV. **Responsibilities**

1. Agency Directors shall ensure that each of their employees, who have access to classified data stored on systems or computer device(s) sign[1] a confidentiality and nondisclosure agreement, which is kept in the employee's personnel file. Vendors who have access to confidential or personal data stored on systems or computer device(s) will sign a confidentiality and nondisclosure agreement prior to the commencement, and prior to any renewal of their contract(s). This agreement shall include the following provisions.

[1] Best practice: The signed confidentiality forms could be more specific than the provisions described in IV 1 a-d (e.g. authorizing access to particular applications' screens) according to agency needs.

a. Computer devices provided by the State and the information stored on them, are the property of the State. The devices and the information are entrusted to employees for safekeeping and use during the performance of their duties.

(i) Employees will understand which data are to be safeguarded.

b. Employees will not disclose, copy, or share data in their custody except as authorized in writing by their supervisors.

c. No form of classified information, on any type of computer device, may be copied to a portable computer device unless all of the following apply:

(i) The information is transferred to a device owned by a state entity or explicitly approved to store state data;

(ii) The information is transferred to a device safeguarded by mandatory, complex passwords and encryption, which meets OIT approved standards;

(iii) To minimize the risk of loss of data, employees will ensure all data stored on their laptop are within folders (e.g. My Documents) which are backed up;

(iv) Written permission specifying the confidential or personal information to be removed is received from the employee's supervisor (in making this decision, the supervisor will consult the data's classification).

d. The supervisor must approve in writing employees copying personal, privileged or confidential information to computer devices owned by employees.

2. A copy of the confidentiality and nondisclosure agreement shall be included in the employee's personnel file, or other approved agency security files, and shall be reviewed and updated annually during the employee's performance review. Each employee shall realize and fully understand that they remain personally responsible for ensuring the safety of computer devices and information, and any loss may result in disciplinary action, personal fines or other action resulting from due process of the law.

V. **Guidelines & Procedures**

A. Any employee who suspects that the integrity or confidentiality of any information entrusted to them, or to a colleague, or a business partner, has been compromised, shall be responsible for immediately alerting their direct supervisor.

B. Any supervisor who receives information regarding the potential breach of classified information shall immediately contact the OIT Customer Solutions Center, who shall, in turn, inform the Enterprise Information Security Officer. The Officer shall promptly work collaboratively with appropriate the Agency Information Technology Director and other technical experts to determine the appropriate course of action.

C. The Office of Information Technology will establish standards and mechanisms to allow recovery of data stored on laptops and personal data assistants.

VI. **Definitions -** See policy.

VII. **References**

A. 5 M.R.S.A. Chapter 163 § 1973. Responsibilities of the Chief Information Officer, paragraph 1B *"Set policies and standards for the implementation and use of information and telecommunications technologies, including privacy and security standards…"*

B. Appendix I Sample OIT Confidentiality and Nondisclosure Agreement

C. 5 safety tips for using a public computer
http://www.microsoft.com/athome/security/privacy/publiccomputer.mspx,

D. 7 ways to protect your laptop on the road
http://www.microsoft.com/athome/security/privacy/ontheroad.mspx, and

E. 4 Ways to Protect Your Mobile PC Against Data Loss and Theft
http://www.microsoft.com/atwork/stayconnected/protectpcdata.mspx

VIII. **Document Information**

Initial Issue Date: April 3, 2007

Latest Revision Date: December 9, 2014 – to update Document Information.

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT, 207-624-8836.

Approved By: Richard B. Thompson, Chief Information Officer

Position Title(s) or Agency Responsible for Enforcement: Kevin St. Thomas, Enterprise Information Security Officer, OIT, 207-624-9845.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1) B and (1) D, which read in part, "The Chief Information Officer shall:" "Set policies and standards for the implementation and use of information and telecommunications technologies…" and "Identify and implement information technology best business practices and project management."

10. Waiver Process: See the Waiver Policy[2]

[2] http://maine.gov/oit/policies/waiver.htm

Appendix I: SAMPLE

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

It is essential and critical that all employees of Office of Information Technology having access to systems, files, data, or documents, provided by the Office of Information Technology, realize that many of these elements contain information relating to either Federal or State data, much of which is confidential in nature. For example, Maine Revenues Services, the Department of Human Services, Motor Vehicle, the Bureau of Employee Relations, to name only a few, are agencies regulated by Federal and/or State laws pertaining to disclosure of information.

Therefore, it is essential that all Office of Information Technology employees agree to recognize and conform to the following policies:

1. No employee shall disclose information relating to any data or information file accessed, viewed, provided by the Office of Information Technology or otherwise entrusted to their keeping.

2. No form of data - source documents, input, hard copy, magnetic tape or disk, or other media - shall be removed from Office of Information Technology immediate possession, by anyone or another State employee, without written authorization by either the Director or Deputy Director of the Office of Information Technology.

3. All data accessed, viewed or provided by the Office of Information Technology is the property of the Office of Information Technology. Requests for copies, extracted data, etc., can only be authorized by the department that originally supplied it. All authorizations granting copy, extracting, or other permission must be in writing prior to release of the information.

4. Office of Information Technology employees will make every reasonable effort to protect the integrity and the confidentiality of data accessed, residing or entrusted to them.

5. Each Office of Information Technology employee realizes and fully understands that unauthorized disclosure or removal of information in any form may result in disciplinary action, personal fines, imprisonment, or other action, resulting from due process of the law.

6. Any employee who suspects that the integrity or confidentiality of any information entrusted to them or the Office of Information Technology has been compromised is responsible for immediately notifying the Agency Information Technology Director, the Enterprise Information Security Officer, and/or the Chief Information Officer.

ALL OFFICE OF INFORMATION TECHNOLOGY EMPLOYEES HAVING ACCESS TO INFORMATION SUPPLIED BY THE OFFICE OF INFORMATION TECHNOLOGY ARE REQUIRED TO READ AND SIGN A COPY OF THIS MEMO INDICATING ACKNOWLEDGMENT AND UNDERSTANDING OF THE ABOVE.

_____ _____

Employee Signature Date